The Evolution and Impact of Blockchain Technology in Various Industries and Regions

[1]Siddharth Rawat, [2]Sarthak Rawat, [3]Piyush Mudgal, [4]Vivek Chauhan, [5]Ritu Pahwa
1,2,3,4 Student, Dronacharya College of Engineering Gurugram, Haryana, India
Head of Department CSE(AIML) and Associate Professor, Dronacharya College of Engineering Gurugram, Haryana, India

[1]siddharth.26385@ggnindia.dronacharya.info, [2]sarthak.24269@ggnindia.dronacharya.info
[3]piyush.24248@ggnindia.dronacharya.info, [4]vivek.24293@ggnindia.dronacharya.info,
[5]ritu.pahwa@ggnindia.dronacharya.info

Abstract— ***Blockchain technology has seen a meteoric rise in not only its development but in its application as well. It is a digital public, the immutable ledger which records online transactions in the absence of a central authority. The past decade has seen blockchain technology revolutionize the world of finance, politics, and stock exchange, and has set a foundation for how transactions will work in daily life. However, technology still poses various problems. Scalability, lack of regulation, and blockchains' anonymous nature of functioning are just some of the drawbacks it faces. Improving the consensus protocols and establishing tighter regulations are a few ways of tackling these problems. Applications of this technology have also been implemented in India in governance, cybersecurity, banking, finance, etc in collaboration with private and government sectors. This research paper gives an extensive overview of the chronology of blockchain and will delve deeper into its impact and its expansion in different parts of the world throughout the past few decades.***

Index Terms—*Blockchain, Chronology, Algorithm, Impact, Expansion*

I. INTRODUCTION

Cryptocurrency and NFTs are most commonly used in this modern era. As we are aware that a cryptocurrency is a form of decentralized currency and NFTs are a form of digital art. Technology that describes these two collectively, is blockchain technology.

In other words, blockchain technology is a chronological chain of blocks with some kind of data in each block and once the block is verified and added to the longest chain, it cannot be deleted or edited.

Most people believe that Satoshi Nakamoto or a group of people named Satoshi Nakamoto invented the technology but this is not entirely true. It was two professors, Stuart Haber and W. Scott Stornetta, who envisioned blockchain technology. Initially, it was a chain of blocks secured with cryptography so that it could resist any possible ways that could change the timestamp of documents. In 1992, it was upgraded with the addition of Merkle trees, which played a major role in enhancing its efficiency by allowing it to store more data on a single block. However, it was in 2008 when the technology evolved and the first blockchain was given to the world in the Name of ‘bitcoin’. In 2009, an official white paper on bitcoin was released as' bitcoin: a peer-to-peer electronic cash system 'by Satoshi Nakamoto[1], where he stated ‘it is electronic cash that a user can send directly from one account to another without any authoritarian means.” The major objective is to have a decentralized system where every transaction is transparent and with no control by any centralized authorities. In 2008, the whole world was shocked by the biggest stock market crash which ended up vanishing 57% of the money from the whole market. This scenario raised a question about the whole centralized system - who was responsible for the People’s money.

II. BLOCKCHAIN STRUCTURE

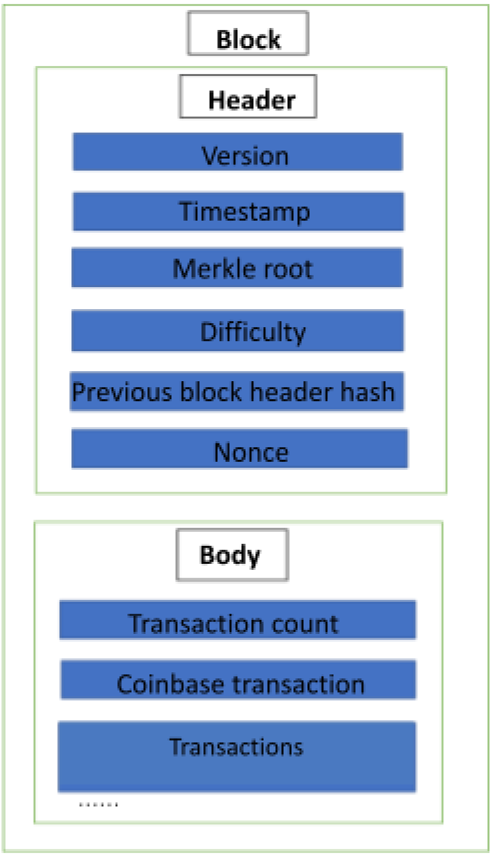
Every block in the blockchain is divided into two parts, block header, and block body. The Block header contains Software Version Number, Timestamp, Merkle root, Difficulty, Previous block header hash, and Nonce. The block body contains the Transaction Count and Transactions as shown below.

Software Version Number: This number Holds Little Value in most cases but is useful for a miner to conclude which protocol decisions it supports.

Timestamp: It gives the time date, hours, minutes, and seconds of when the block was created since 1970–01–01 T00: 00 UTC

Merkle Root: All transactions inside a block are aggregated to a hash known as the Merkle root. Further elaborated in section 5.

Difficulty - It indicated the size of the new hash required to claim validity i.e., the number of strings of zeros required at the beginning of the hash to be validated.



Blockchain Structure
fig (1)

Previous Block Hash - The hash/digest of the previous block in the blockchain. The only exception is the genesis block.

NONCE - NONCE (Number Only Used Once) is a number added to a hashed blockchain that meets the difficulty level restrictions when rehashed. [3]

Transaction - The block body contains all transactions that are confirmed within the block.

Transaction Count - This contains the number of transactions inside the block.

A. *Blockchain Mechanism*

A block is a public, decentralized, immutable, digital ledger that records transactions. The first block in every blockchain is known as the genesis block, and a series of these chronologically connected blocks make up a blockchain. For a transaction to be valid in a block, it needs to be authenticated and verified. Here is where the concept of digital signatures comes into play. Digital signatures are the fundamental building blocks in blockchain technology, whose main purpose is to authenticate transactions [12]. Every user who wishes to participate in this peer-to-peer transaction system must first create a public key/private key pair whose date is formatted into some strings of bits. Producing a digital signature requires a function that takes the transaction message and the users' private key as input to ensure that only that specific user can produce the signature. The transaction message ensures that each transaction has a unique signature, so it can't be applied to a different transaction message. Added to this is another function that verifies the validity of the digital signature. This function takes the transaction message, the public key, and the signature produced from the previous function and outputs true or false based on the validity of the signature. Bitcoin currently uses the ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm to verify digital signatures. Hence Through this protocol, the validity of a transaction is verified.

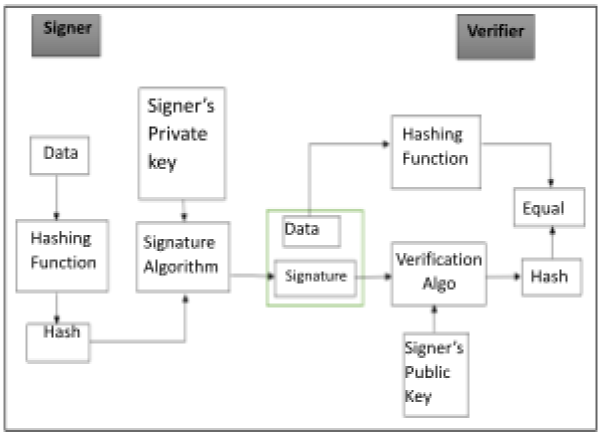


fig (2)

Since bitcoin is a decentralized system, each member participating in the network maintains their sequences of transactions (blockchains). An algorithm called the consensus algorithm is used to verify which transactions are rejected and which will be added to the blockchain.

B. *Consensus Algorithms*

A consensus algorithm is a protocol that allows all blockchain members to agree on which transactions should be recorded onto the block and reach a consensus on the current state of the blockchain. There are numerous consensus algorithms available, Proof of Stake (PoS), Proof of Work (PoW) [7], Proof of Authority (PoA,) and Delegated Proof of Stake (DPoS), are some examples [2]. The PoW consensus algorithm is currently used by Bitcoin, Ethereum, and Litecoin. Miners guess and check for the proper hash value, and once the hash is found, the block is mined and the transaction is validated. The PoW protocol uses a cryptographic hash function called SHA-256, which takes the data stored in the block as input and assigns it a unique number. Following is the working of cryptographic hash functions [6]. A cryptographic hash function is a function that can take any arbitrary input, such as a message or a file, and return a string of bits with a fixed length called the digest or the hash value [1][4]. This function always returns the same output for the same input and cannot be reverse-engineered to obtain the original input [4]. The most common hash functions are SHA-2, SHA-3, SHA-256, MD5, BLAKE2, and so on. SHA-256 is the most popular hash function because of its predominant use in blockchain technology [5]. The digest created using this function is stored in the succeeding block as well as in the block itself. A NONCE is added at the end of the block, after which applying the SHA-256 hash function gives a string of bits whose beginning contains a specific number of consecutive 0s, which verifies PoW.

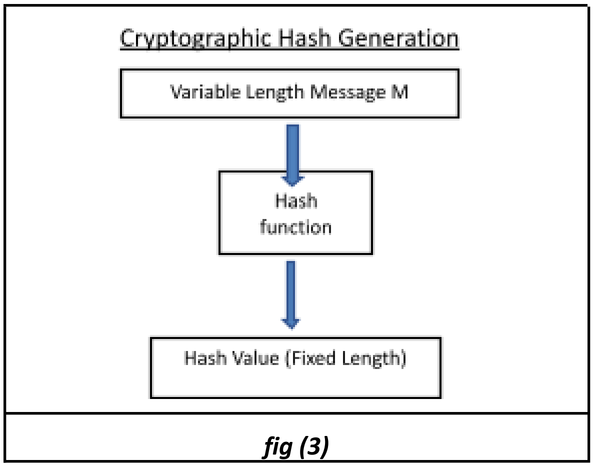

Cryptographic Hash Generation
Variable Length Message M
Hash function
Hash Value (Fixed Length)

fig (3)

C. *Mining and Block Rewards*

Mining in blockchain technology is the process by which transactions on the blocks are validated and added to the blockchain ledger [1]. It is done so by solving cryptographic hash puzzles to verify the validity of the transactions recorded in the blocks [8]. The Bitcoin protocol allows anybody to be a block creator. A block creator, also known as a miner, listens for broadcasted transactions, compiles them into a block, and computes the NONCE, upon which applying the SHA-256 algorithm gives a string of bits with the desired number of zeros at the beginning.

The number of zeros at the beginning of the hash increases over time to make computing the correct hash more difficult. This guarantees that as the number of miners increases and technology advances, a new cryptocurrency will be added to the economy at a steady rate. Upon finding NONCE, the block is validated and the miner broadcasts the block to all the peers in the network, and every individual updates their blockchain. To reward the miner for their work, the miner is given a certain amount of cryptocurrency, and the new currency is added to the economy. Next, we will discuss how data is encoded efficiently and securely.

D. *Merkle Tree*

A Merkle tree, also known as a hash tree, is a data structure composed of hashes of distinct data blocks that function as a summary of all the transactions in a block and also allow for the secure and efficient confirmation of large data sets.

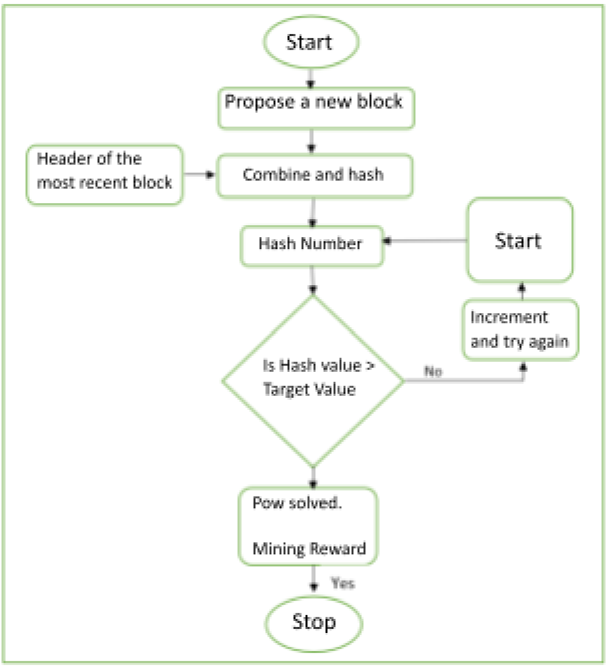
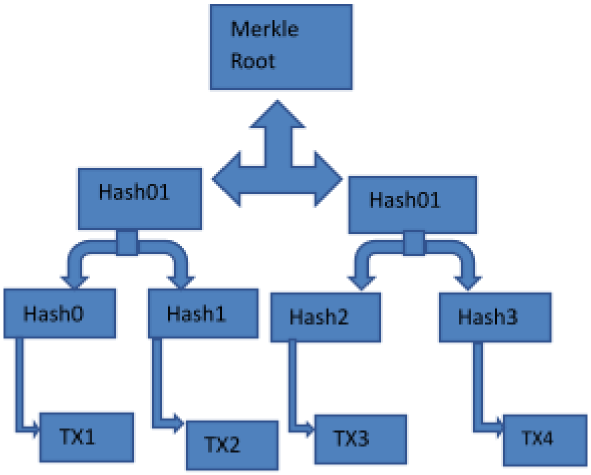


fig (4)

The Merkle tree also aids in the verification of data consistency and content. Bitcoin and Ethereum both use Merkle trees [9]. A Merkle tree creates a digital fingerprint of the entire set of transactions to record all transactions in a block. It allows the user to determine whether a transaction can or cannot be included in a block. Merkle trees are formed by hashing pairs of nodes repeatedly until one hash remains [9]. The Merkle Root, or Root Hash, is the name given to this hash. Merkle Root appears in the block header. The block header is the portion of the bitcoin block that is hashed during mining. The Merkle tree is useful because it allows you to keep the integrity of the data. It conserves memory or disc space, and its proof and management necessitate only a small amount of data to be transmitted across networks.



fig(5)

III. IMPACT OF BLOCKCHAIN TECHNOLOGY

The twenty-first century is seeing astounding technological advancement, especially in information technology. Recent talks about AI technology, machine learning, blockchain, and everything that depends on it demonstrate the impact of technological progress. The "fad" of blockchain is catching up in terms of the currencies that have sprouted from it, as well as the underlying technology to achieve clarity and immutability. According to publicly available data, Indians have also invested in cryptocurrencies valued at more than USD 10 billion. And apart from that, we can see that the technology involved has found a large number of adopters in the banking and financial sectors.

Multiple businesses in the private sector are exploring blockchain to make it more efficient, and as a result, they are attempting to revisit their internal processes and workflows to add value to their existing systems. More than half of industries in India are integrating blockchain technology into their organizational systems. The National Informatics Centre has created a Blockchain Technology Centre of Excellence (CoE), which will serve as the nation's coordinated, integrated blockchain ecosystem. Blockchain technology is impacting many sectors.

A. Cryptocurrency

Cryptocurrency is one of the most popular applications of blockchain technology. It is a form of decentralized currency that uses blockchain to store the number of immutable transactions in a single block. Some examples of cryptocurrencies are: -

- Ethereum

It is one of the most popular cryptocurrencies after Bitcoin in terms of trading and number of uses. It is based on one of those blockchains that provide a platform for users to build through smart contracts. Users can build Dapps, which stands for decentralized applications.

- Solana

Solana is considered one of the fastest cryptocurrencies because it provides more transactions as compared to Ethereum. If we talk about numbers, it lets users transact 65000 transactions in one second, and for Ethereum, it gives 30 transactions in one second.

- Litecoin

Litecoin has shown its importance in the market through its innovative blockchain technology. It uses a different algorithm called "script", which is considered to be one of the latest algorithms, whereas Bitcoin uses the SHA256 algorithm.

1. Trading Cryptocurrency.

The price of any cryptocurrency, like any other trading asset, is determined by supply and demand. Still, what distinguishes it from other assets is that it is decentralized, making it volatile to trade. Its price fluctuates with each second. One example of its volatility is "Terra (Luna)," which went from a $400 billion valuation to a $500 million valuation in a matter of hours. Many well-known people who had invested in it lost the majority of their profits. KSI, a well-known YouTuber who had invested more than $3 million, lost everything in this crash.

Here, fig. 6 shows the fall of Terra (Luna).

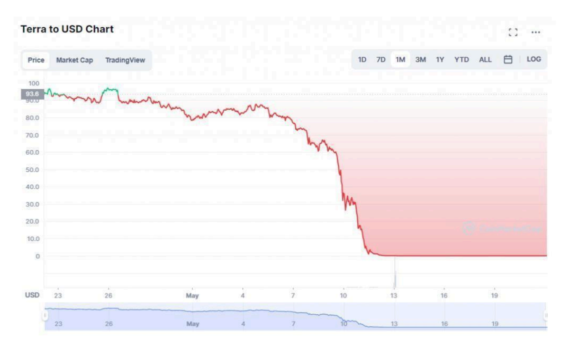


Fig. 6

Volatility might be a negative factor but El Salvador, a country in Central America, adopted bitcoin to help its economy and to increase domestic consumption. But on the other hand, China has already banned the trading of cryptocurrency allegedly saying that it promotes mischievous activities, and launched its official cryptocurrency called “e-yuan”.

India had a different reaction to cryptocurrency; India has decided to impose a 30% tax on the profit earned by trading crypto as income from other sources and an 18% tax on the companies providing the services of crypto trading.

B. DAOs

Decentralized autonomous organizations (DAOs) are a group of people, wherein a decision every vote counts, and members who had bought or invested in the currency or token can give a vote. This system is still in its earlier stage with lots of issues of security, but according to the experts in the corporate and business world, DAOs can be beneficial if used with a combination of online and offline authoritarian supervision.

C. Securitization

Blockchain is considered by market participants as a technology that helps to reduce the need for cognition and due care by enhancing reports and monitoring them using immediate access to unchangeable data, excellent implementation, as well as making new kinds of assets and lowering base barriers and structures through facilitation.

D. Payments and settlements

Usage of blockchain to reach efficient transaction activities, circulation, and enforce business requirements, cutting costs by removing middlemen and simplifying the infrastructure, reducing data leakage, and improving the clarity and regularity from beginning to end.

E. Intercompany settlements

The ability of blockchain to preserve a single source of undisputed fact, digitize intercompany transfers using decentralized applications, and provide access across disparate systems and consensus mechanisms significantly reduces inter-company imbalances and costs. Leveraging near-real-time reporting rather than the period-end streamlining and normalizing intercompany supply chain processes would also revolutionize intercompany relationships and supply chain processes.

F. Digital assets custody

Product development as well as vendor selection for cryptocurrency custody; accounting as well as the tax treatment of cryptocurrency transactions in changing environments; capital controls evaluations; cybersecurity; and controls development.

G. Syndicated loans

Improving implementation and fixing effectiveness across the syndicated loan ecosystem by implementing smart contracts to regulate terms and services of loans, distributed ledger technology to address transaction tracking and communication issues, and transparent and unchangeable data to shed more light on time-consuming reconciliations and erroneous payments.[13].

H. NFTs:

Non-fungible tokens (NFTs) enable financial markets to represent tangible assets on a blockchain. Enterprises are attempting to determine a way to maximize the profit that tokenization and NFTs have the potential to improve core operations and financial products[14]. Smart contract testing:

Smart contracts are a critical component of blockchain applications. Blockchain tech users must test smart contract code for precision, security, uniformity, and efficiency [13]. It is also critical to examine the features, functions, and control mechanisms that surround the applicability. Finally, end-users of Blockchain technology must conduct continuous improvement testing.

G. Blockchain technology in Indian sectors

"Blockchain" has emerged as having the potential to revolutionize many elements of how the public and Private/commercial sectors conduct business. Its potential has been recognized globally, with many international organizations and technology companies emphasizing the benefits of its application in lowering operational and compliance costs while also improving efficiencies. Blockchain has tremendous potential to solve real-world problems for businesses, governments, and users in emerging economies like India.

1. *Government Sector.*

Surprisingly, the involvement of the government of India is way more than the big businesses and tech giants in India, appreciating the potential of the technology and using it for the benefit of the people of India. Major government projects that include blockchain technology as their foundation are as follows:

1) CBDCs (E₹)

Central Bank Digital Currencies (CBDCs), also known as Digital Rupee (E₹) is a digital form of the Indian Rupee which means it is like a physical rupee note except it is in digital form, released by the Reserve Bank of India (RBI CBDC is defined broadly by the RBI as digital legal tender issued by a reserve bank. It is similar to sovereign paper currency but has a different form, is tradeable at the same rate as existing currency, and will be accepted as a form of payment.

CBDCs use a Private blockchain chain making it scalable as it uses a permission-based network easier for the RBI to keep track of transactions, increasing transparency, and allowing for real-time tracking and ledger maintenance. Since RBI maintains it, hence providing the uses of private virtual currency without the risks.

The Digital Rupee is considered to be a progressive step towards the Digital India vision.

2) Land Registry

The land ownership and transfer system in India was largely inherited from the British administration, and it is primarily established through a registered sale deed, which is not a government-assured title to the property. The National Institution for Transforming India (NITI) Aayog discovered during a pilot project that establishing possession over land and maintaining land records is complex, with inconsistencies and disputes having to compromise a huge amount of matters pending before various administrative and judicial forums. Poor land record maintenance, high levels of litigation, and information across different agencies were recognized as major concerns in the land transaction process.

To address these concerns, NITI Aayog and its technology partner devised a process flow to manage land record transfer and ownership and to identify specific blockchain features that could be used to streamline the process. The process was found to be greatly simplified by the decentralized nature of blockchain technology and its capacity to carry out smart contracts. To demonstrate the capabilities of a redesigned system built on top of a blockchain, a prototype was created. This prototype allowed citizens to manage their land transfer (including uploading necessary documents and payments through a single user-friendly portal) and to view the status of their transactions through events immutably stored on the blockchain.

3) Pharmaceutical drugs supply chain

The pharmaceutical industry faces Numerous issues, such as supply chain management inefficiency, lack of transparency, and counterfeiting. The Indian government has put into place several initiatives to address these problems, including the use of distinctive identification codes and a track and trace system. These remedies haven't entirely been successful in resolving the issues, though.

Many of the problems that the Indian pharmaceutical industry is currently facing could be solved by blockchain technology. It can increase the reliability, efficiency, and transparency of transactions and provide full traceability of pharmaceutical drugs, making it easier to optimize drug flow and implement an effective inventory management system, which will significantly improve stock planning. By enabling the accurate identification of drug locations at each point of transaction and the efficient sending of "batch reminders" to ensure patient health safety, blockchain also improves transparency and accountability.

The government can take the lead in enabling a common public infrastructure built on top of an underlying blockchain system that would also significantly benefit various government schemes in the health sector by reducing dependence on the financial intermediary, ensuring transparency in stock movement, controlling quality, and enhancing the industry's reputation in general. In general, the adoption of blockchain technology in the Indian pharmaceutical sector has the potential to have a significant positive impact on both the sector and the general public.

4) SuperCert: anti-fraud identity intelligence blockchain solution for educational certificates

With over 7,500 organizations offering phony employment and educational credentials, paper-based certification in India is vulnerable to fraud and manipulation. While ethical organizations carry on, the University Grants Commission (UGC) frequently blacklists universities and organizations. Companies are spending a lot of money to verify credentials, and students must go through laborious and time-consuming procedures, which adds significantly to the cost of the issue.

In India, the system in place for verifying educational credentials is centralized, labor-intensive, manual, and subject to fraud and tampering. SuperCert, a blockchain-based solution, was created by NITI Aayog in collaboration with the Indian School of Business (ISB) and Bitgram to address these issues. SuperCert is a permission-based blockchain architecture that issues and verifies diplomas using intelligent identity interlinking and encryption. A block of student certificates must be created, a unique blockchain representation of each student's identity must be created, and the certificate must be verified using both the student and the university's public keys.

The immutability of blockchain technology makes it impossible to tamper with the certificate. SuperCert is a real-time, automatic, fraud-proof, and tamper-proof solution for educational certificate verification because it offers features for both online and offline verification.

5) EV Battery Swapping

By 2030, the Indian government wants 30% of all vehicles to be powered by electricity. However, obstacles to achieving this goal include the high cost of usage and the limited driving range of the vehicles. In addition, there is a problem with the inadequate infrastructure of charging stations required for the widespread use of EVs. The creation of battery-sharing ecosystems that would enable users to swap batteries out when they ran out of charge rather than relying on charging stations has been proposed as a solution to this issue.

Battery-sharing ecosystems may find solutions to their problems using blockchain technology and the Internet of Things (IoT). An immutable record of battery information, such as age and previous treatments, can be provided by the use of blockchain, preventing misrepresentation to drive up or drive down the cost of use. The use of programmable transfers in this context is another potential blockchain application. Simple rules on costing based on battery attributes could be implemented using smart contracts, which are self-executing contracts in which the terms of the agreement between the buyer and seller are directly written into lines of code. This would make switching out batteries at charging stations more effective.

6) Securities and Exchange Board of India(SEBI)

All depositories in India are required by SEBI (the Securities and Exchange Board of India) to use blockchain technology for record-keeping. With this action, record-keeping, and monitoring the creation of securities will all be more transparent. Because they keep track of all the securities that investors own, depositories play a crucial role in the securities market. Because blockchain technology offers a safe and impenetrable method of storing and sharing data, it is anticipated that its use in record-keeping will increase transparency and efficiency.

The decision by SEBI to use blockchain technology for record-keeping is consistent with a global trend toward its use in the securities market. The use of blockchain technology is being investigated by numerous nations, including the US, UK, and Japan, to increase the effectiveness and accountability of their securities markets.

Overall, it is anticipated that the securities market in India will become more transparent, efficient, and secure thanks to the use of blockchain technology in record-keeping, which will eventually benefit investors and other stakeholders.

7) Agriculture

A Blockchain-based system for fertilizer subsidies has been developed by NITI Aayog in partnership with Gujarat Narmada Valley Fertilizers & Chemicals Limited (GNFC). The Directorate of Agriculture in Jharkhand and SettleMint, an international blockchain technology company based in India, jointly announced the effective launch of a seed distribution program for farmers based on blockchain technology. This will make seeds timely available to retailers, wholesalers, and most importantly, farmers.

2. Private sector

Impact of Blockchain Technology is not limited to the schemes and policies of Government sectors, it also expands its horizon to create a boom in the startup world of India, where startups leverage the technology and create various innovative ideas by offering new ways to solve traditional problems and creating new opportunities and also improving the overall startup and entrepreneurial culture in India.

Top Tech giants and business leaders in different fields directly or indirectly, are trying to connect with this technology, one of the ways is by directly investing in them, some of the innovative startups are given below:

1) Signzy

Ankit Ratan, Arpit Ratan, and Ankur Pandey founded Signzy in Bangalore in 2015 as a digital banking infrastructure that combines AI and blockchain to produce user-friendly, legal products that put safety first. In 2018, it received Series funding totaling more than $3.6 million.

2) InstaDapp

Founded by Sowmay Jain in Bangalore, InstaDapp is a DeFi infrastructure that enables developers to fully realize the potential of the technology by facilitating app creation and encouraging interoperability between various DeFi blockchain protocols. It is based on the Ethereum blockchain. People can borrow and lend money, as well as earn interest on their savings.

3) KoineArth

Founded by Praphul Chandra, KoineArth's Nash platform offers customizable solution frameworks for a variety of actual blockchain use cases. It is a Blockchain- and AI-based solution that is compatible with ERP and enables businesses to work together to build networks, markets, and economies with reliable information and financial incentives.

4) Matic Network

Bringing the world to Ethereum, Matic Network was established by Jayanti Kanani, Sandeep Nailwal, and Anurag Arjun in Bangalore in 2019. A decentralized Ethereum scaling platform called Polygon enables programmers to create user-friendly, scalable decentralized applications (dApps) with low transaction costs without compromising security. Polygon has been used to scale the performance of more than 7000 dApps.

5) WazirX

An Indian cryptocurrency exchange and trading platform, WazirX was established by Nischal Shetty in Mumbai in 2017. It introduced the Smart Token Fund (STF), a community-driven initiative that enables cryptocurrency enthusiasts to connect with knowledgeable traders and increase their cryptocurrency portfolios on WazirX, as well as the ground-breaking open-sourced blockchain project Shardeum.

6) MindDeft

Established in Ahmedabad by Krunal Soni in 2015, MindDeft specializes in blockchain apps and links companies to the decentralized world by utilizing the potential of blockchain. Among their services are the creation of cryptocurrencies, smart contracts, token sales, private blockchains, distributed ledgers, and legal contracts.

7) Somish

Ish Goel founded Somish, one of India's most rapidly expanding blockchain startups, in New Delhi in 2006. It uses blockchain technology in partnerships with Fortune 500 companies, governments, and startups to create market-leading products that have won awards.

8) Primechain

Primechain is a new Indian blockchain startup to create blockchains for a better world. It was founded by Shinam Arora in Bangalore in 2016. In less than six minutes, its blockchain ecosystem is fully functional and includes a web application, a mobile Progressive Web App, and a Blockchain REST API service.

9) PSI PHI Blockchain Lab

The PSI PHI Blockchain Lab was established in Bangalore in 2016 by Gaurav Kumar, Aditya Prasad, and Harsh Pokharna. The lab creates blockchain-based document storage solutions. It focuses on the healthcare and supply chain sectors and plans to usher in a new era of products that combine cutting-edge technology with human interaction.

IV. DRAWBACKS AND SOLUTIONS OF BLOCKCHAIN TECHNOLOGY

A. *Scalability Issue*

Simply put, the more individuals connect to the network, the more likely it will slow down. However, more and more changes are taking place in the way blockchain technology works. This is good technological advancement, and scalability alternatives are also incorporated into the bitcoin network. The answer is to conduct transactions outside of the blockchain and utilize the blockchain to store and retrieve information. A permission network or the use of another architectural blockchain solution like Corda are two more innovative ways to control scalability. However, not all of these solutions can scale to the same levels as centralized systems. Transaction speeds between Bitcoin and VISA are vastly different from one another [15]. Only 4.6 transactions can be completed with Bitcoin at the moment. VISA can process 1700 transactions per second, in contrast. This indicates that 150 million transactions can be completed in a single day. Finally, it's possible that blockchain isn't yet suitable for practical uses.

The process of verifying transactions becomes more complex and difficult as the popularity of cryptocurrency increases because mining requires more computational capacity. Every transaction necessitates transaction fees [16]. If you want your payment to be validated faster, you can pay a higher fee. As the network grows, many new users expect their transactions to be processed immediately. As a result, there are many unverified transactions in the queue awaiting validation. As a result, scalability decreases [16].

B. *Energy Consumption*

Blockchain technology was initially introduced with Bitcoin. It employs the decentralized consensus mechanism known as PoW (Proof-of-Work), which relies on miners to carry out laborious work. The miners are urged to work out challenging mathematical puzzles. These difficult mathematical puzzles are not ideal for the actual world due to excessive power usage[15]. The largest cryptocurrency in the world, Bitcoin, currently uses more than a small nation's yearly electricity consumption, or about 150 terawatt-hours (TWh). Bitcoin requires computers to tackle increasingly difficult math problems to verify transactions. Significantly more energy is used by this proof of work consensus mechanism[17].

C. *Security Issues in Blockchain*

51% Attack: It is an attack that is done on the blockchain by a single person or group of people who controls more than 50% of the mining hash rate of the network. The attackers can cease the execution of new transactions and even confirmations. Malicious operators can then rewrite sections of a blockchain and reverse transactions. A 51 percent attack typically gets around the blockchain's data encryption [18]. The impact of attacks can be light or intense; it depends on the mining power of the attacker.

The 51% attack heavily influences the computing resources of the miners. This may slow down the transactions to be confirmed so that they can be stored in the blocks. Consequently, the blockchain network gets deprived, and this allows the attackers to process all the transactions much faster than the miners.

The 51% attack authorizes the attackers so they can reverse the transactions even before they have been confirmed. This leads to the problem of double-spending a coin. Due to this somehow, the actual minors receive less to modernize the blockchain as the attackers take away their portions or shares.

Some big blockchain platforms like Bitcoin and Ethereum are less likely to be attacked by the 51% attack as they need a lot of high hashing power. For this reason, the 51% attack is limited to small cryptocurrencies. Many small cryptocurrencies are affected by the 51% attack.In May 2018, Bitcoin Gold, a cryptocurrency, was attacked by a 51% attack. As a result of this, more than 50% of the hash power is controlled by the attackers, and this enables the attackers to double-spend for many days, at the cost of stealing over $18 million worth of Bitcoin Gold. Then, later in 2020, Bitcoin Gold was again attacked by the 51% attack. Ethereum Classic, another cryptocurrency, suffered from three different 51% attacks in one single month. The first one took place on August 1, the second one on August 6, and the third one on August 29. The founder of Ethereum, Vitalik Buterin, stated that this is a disadvantage of PoW networks, noting that Proof–of–Stake (PoS) networks are less vulnerable to attack.

D. *Private Key Dependency*

For blockchain to be decentralized, individuals must be able to act as their bank. This, however, leads to another issue.

To access the user's assets or information stored in the blockchain, a private key is necessary. The user should keep track of it. It is generated throughout the wallet-building procedure. Additionally, they must ensure that nobody else has access to it. Their wallet will be in jeopardy if they do otherwise. Access to the wallet is simply lost when a private key is lost. One of the main drawbacks of blockchain is its dependency on people [19]. As a result, if you misplace your private key, your wallet will be locked and unable to be accessed again. Since not all users are digitally skilled and are more likely to make errors [19]. If a centralized authority is in charge of it, the goal of decentralization is defeated.

E. *SOLUTIONS*

New blockchains were constantly getting built to resolve the problems, for example, EOS which uses 0.0011 TWh makes it 66000 times more energy efficient than bitcoin and almost 17000 times Ethereum. Monero Zcash and Dash with better security protocols and fewer computational equipment requirements which makes them more secure and Scalable respectively. Better consensus algorithms like Proof of stack are being used by blockchains like Ethereum to achieve distributed consensus and conquer the issues with the previous algorithm, Proof of Work.

V. CONCLUSION

Blockchain technology has made significant strides in the past decade, impacting various industries and regions around the world. While its origins lie in the world of cryptocurrencies like Bitcoin, the underlying distributed ledger technology has found applications spanning finance, governance, supply chains, and more. The immutable and decentralized nature of blockchains provides transparency, security, and trust in record-keeping and transactions.

However, the technology is still in its nascent stages and faces several challenges that need to be addressed. Scalability issues limit the number of transactions that can be processed, and the high energy consumption required for mining operations is a concern. Security vulnerabilities like 51% attacks and private key management pose risks that must be mitigated. Lack of regulatory oversight is another area that requires attention as blockchain applications become more widespread.

As the technology continues to evolve and mature, addressing its current limitations will be crucial for blockchain to realize its full potential in revolutionizing transactions, records, and processes across diverse domains. Ongoing research, innovation, and collaboration between stakeholders will shape the future trajectory of this disruptive technology. While challenges remain, the foundations have been laid for blockchain to drive transparency, efficiency, and trust in an increasingly digital world.

REFERENCES

[1] "But how does bitcoin actually work?" *YouTube*, Jul. 07, 2017.

[2] 101 Blockchains, "Beginner's Guide: What is Consensus Algorithm?," *101 Blockchains*, Sep. 29, 2021.

[3] "What is a Nonce in BlockChain?," *What is a Nonce in BlockChain?*, Jun. 15, 2022.

[4] S. E. Team, J. Knudsen, J. Rabon, and C. Purandare, "What are cryptographic hash functions? | Synopsys," *Application Security Blog*, Dec. 10, 2015.

[5] "Blockchain Hash Functions - Javatpoint," *www.javatpoint.com*. , Jun. 15, 2022.

[6] "Consensus Algorithms in Blockchain GeeksforGeeks," *GeeksforGeeks*, Apr. 25, 2019.

[7] L. Daly, "What Is Proof of Work (PoW) in Crypto? | The Motley Fool," *The Motley Fool*, Sep. 27, 2021.

[8] "What Is Bitcoin Mining: How Does It Work, Proof of Work and More | Simplilearn," *Simplilearn.com*, Apr. 19, 2019.

[9] "Blockchain Merkle Tree - Javatpoint," *www.javatpoint.com*.

[10] "Block - Bitcoin Wiki," *Block - Bitcoin Wiki*. https://en.bitcoin.it/wiki/Block (accessed Jun. 15, 2022).

[11] M. Vidrih, "What Is a Block in the Blockchain? | by Marko Vidrih | DataDrivenInvestor," *Medium*, Feb. 22, 2019.

[12] Bhargavi K. Chauhan, Dhirenbhai B. Patel, "A Systematic Review of Blockchain Technology to Find Current Scalability Issues and Solutions", Proceedings of Second Doctoral Symposium on Computational Intelligence, vol.1374, pp.15, 2022.

[13] " Building a better working world | EY &ndash; the US," *EY US - Home | Building a better working world*, May 12, 2022. www.ey.com (accessed Jun. 16, 2022).

[14] "Student paper." https://www.ljmu.ac.uk/microsites/library/researcherengagement-and-outputs/ljmu-e-theses-service (accessed Jun. 16, 2022).

[15] " *101 Blockchains*, Jun. 15, 2022. 101 | blockchains.com (accessed Jun. 16, 2022).

[16] "Blockchain Innovation Agency Applicator," *Applicator*, May 09, 2022. applicature.com (accessed Jun. 16, 2022).

[17] "RideAble – Let A Horse Change Your Life," *RideAble*. rideable.org (accessed Jun. 16, 2022).

[18] "Edge as a Service (EaaS) - Flexible Edge Compute Platform | Section," *Section*. www.section.io (accessed Jun. 16, 2022).

[19] M. U. Official Website, "Established By Dr. Nawal El Degwi in 1996 - MSA University," *Established By Dr. Nawal El Degwi in 1996 - MSA University*.